



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/719,303	11/21/2003	Michael Bensimon	886-011604-US(PAR)	3004
2512	7590	02/22/2007	EXAMINER	
PERMAN & GREEN 425 POST ROAD FAIRFIELD, CT 06824			ZIA, SYED	
			ART UNIT	PAPER NUMBER
			2131	
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		02/22/2007	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

**Office Action Summary**

Application No.

10/719,303

Applicant(s)

BENSIMON ET AL.

Examiner

Syed Zia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 21 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>04/04</u> . | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

This office action is in response to application filed on November 21, 2003. Original application contained Claims 1-21. Therefore, presently pending claims are 1-21.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-21 are rejected under 35 U.S.C. 102(5) as being anticipated by Julin et al. U. S. Patent 5,557,679.
2. Regarding Claim 1, Julin teach and describe a method for establishing and managing a trust model between an identification module and a radio terminal, characterized in that it comprises: a terminal authentication step by said identification module; said identification step being carried out by means of identification means provided either to said identification module by a mobile radio-telephony network at the time of an initialization step or similar or at the time of a so-called updating step, or to said terminal by the identification module; a control step by said module of at least one specific characteristic of the terminal, said specific characteristic

Art Unit: 2131

being previously transmitted by radio-telephony to said module from a secured server of said mobile radio-telephony network (Fig.1-3, col.3line 20 to col.4line 26).

3. Claims 2-21 are rejected applied as above in rejecting claim 1 Furthermore, Julin teaches and describes a method of trust mode and personalization a chip card for mobile telephone system, wherein:

As per Claim 2, the lifetime of said terminal authentication means present in the identification module is limited by a determined expiration date, said authentication means being comprised of at least one authentication key (col.4 line 6 to line 16).

As per Claim 3, wherein said identification module is an SIM type chip card or an USIM card for third-generation networks or an equivalent card comprising in a memory the representative subscription data (Fig.3, col.3 line 20 to line 35).

As per Claim 4, wherein the identification module maintains a trust relationship with the radio terminal by generating authentication means and then by providing these authentication means to the radio terminal by secured exchange mechanisms based on authentication means initially available from the radio terminal (col.3 line 30 to line 40).

As per Claim 5, comprising at the time of said initialization or updating step a generation step, carried out at least by said identification module, of a so-called trust key, said trust key being

Art Unit: 2131

used by said module for encrypting at least data exchanged between the identification module and the terminal (col.3 line 55 to col.4 line 16).

As per Claim 6, wherein said initialization step of said authentication means is done on the initiative of the radio-telephony network, after denial of the key initiated by said module or the mobile radio-telephony network or the radio terminal, following an expiration of the validity period of the key or even at the time of initialization of the identification module (col.2 line 15 to line 33, col.2 line 44 to line 65).

As per Claim 7, wherein said authentication step comprises especially the following steps: an utilization step in the terminal of at least one first authentication key memorized in the terminal by at least one first authentication algorithm memorized in the terminal, said first key having a validity period limited by a predefined expiration date; an utilization step by the identification module of utilization of at least one second key memorized in the identification module by at least one second authentication algorithm memorized in the identification module, said second key being identical or complementary to the first key and associated with the terminal, said second key having a validity period limited by said predefined expiration date; a comparison step in the identification module for comparing the results obtained by said first and second algorithms (col.3 line 63 to col.4 line 26).

As per Claim 8, the authentication step comprises the utilization of said predefined expiration date (col.3 line 52 to col.4 line 26).

As per Claim 9, said initialization step is initiated by a mobile radio-telephony network and also comprises: generation by the identification module of at least one of said first and second keys; a storage in the identification module of said second key; transmission to the terminal by the identification module of said first key, said first key being encrypted by use of the trust key (col.3 line 52 to col.4 line 16).

As per Claim 10, wherein said comparison step is done between, on the one hand, a response produced by said first algorithm, stored in memory in the terminal and transmitted to said identification module and, on the other hand, a response result, stored in memory in the identification module, produced by said second algorithm (col.3 line 43 to col.4 line 26).

As per Claim 11, wherein said first key is an asymmetrical private key  $K_s$  and said second key being a public key  $K_p$  complementary to the first key (col.4 line 6 to line 16).

As per Claim 12, wherein said first key is symmetrical, said second key stored in memory in the identification module being identical to the first key, these keys forming a single symmetrical authentication key (col.4 line 6 to line 26).

As per Claim 13, comprising an updating step of said first and second keys, initiated by the identification module prior to said predefined expiration, said updating step including the following sub-steps: authentication between the terminal and the identification module using said

Art Unit: 2131

first and second keys; generation by an updating algorithm of the identification module of at least one updated key taking into account an information for replacing at least one of said first and second keys; memorization in the identification module of the updated key for replacing said second key; transmission to the terminal by the identification module of the updated key analogue of said first key (col.3 line 52 to col.4 line 26).

As per Claim 14, wherein said updating step comprises in addition the control of at least one identifier of the terminal and/or of the identification module (col.3 line 63 to col.4 line 6)

As per Claim 15, wherein an encryption of the key is carried out for said transmission to the terminal of the updated key analogue of the first key, said key encryption being done by said trust key (col.3 line 43 to col.4 line 26).

As per Claim 16, wherein the updating step also comprises the following steps:  
generation by the identification module of a new trust key after said authentication between terminal and module; memorization in the identification module of the new trust key;  
transmission to the terminal by the identification module of the newly generated trust key (col.3 line 43 to col.4 line 26).

As per Claim 17, wherein said updating step is completed by a verification test comprising a return transmission on the part of the terminal of at least one datum representative of effective receipt of data transmitted by the identification module during the updating step

Art Unit: 2131

(col.3 line 43 to col.4 line 26).

As per Claim 18, wherein said trust key is a symmetrical encryption/decryption key analogous or identical to said symmetrical authentication key (col.3 line 43 to col.4 line 42).

As per Claim 19, wherein said trust key is an erasable session key (col.3 line 43 to line 63).

As per Claim 20, wherein a so-called revocation step is carried out on the initiative of the identification module, of the terminal, or of the corresponding radio-telephony network, said revocation step comprising the erasure in a memory of said identification module of at least said first key associated with the terminal (col.3 line 43 to col.4 line 26).

As per Claim 21, an identification module in a terminal for the implementation of the method, characterized in that it comprises means for memorizing at least one authentication key as well as at least one authentication algorithm, calculation means for executing at least one step consisting of applying said authentication key to said authentication algorithm memorized in the identification module, communication means, means for initiating a revocation and revocation means for revoking said authentication key, means for memorizing a specific characteristic of the terminal and means for actuating an updating algorithm for updating said authentication key, the communication means being capable of providing at least one authentication key to the terminal and receiving data send from a secured server of a mobile radiotelephony network (col.3 line 43 to col.4 line 26).



Art Unit: 2131

**Conclusion**


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SZ

February 16, 2007

  
SYED ZIA  
PRIMARY EXAMINER  
Feb 21 2007